IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRIC OF ALASKA

IN THE MATTER OF THE SEARCH OF	Case No.:
Black Smartphone w/ UB Pro Case (FBI Evidence Item 1B-6) Blackberry cellular phone (FBI Evidence Item 1B-7) AT&T prepaid SIM cards- 8901410327159970336 8 and 8901410327178942538 4 (FBI Evidence Item 1B-8)	**(FILED UNDER SEAL)** Jun 09 2020

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Frank D Reid, Jr, (Affiant) being first duly sworn, upon oath, depose and state the following:

BACKGROUND

1. I am currently employed as a Special Agent (SA) for the Federal Bureau of Investigation (FBI), and have been so employed since December 2010. During my employment with the FBI, I have been assigned the investigation of criminal matters within the jurisdiction of the FBI, with emphasis in the areas of drugs, violent crimes, crimes against children, and white-collar investigations. Prior to being assigned to the Anchorage Division, I served an assignment in San Jose, California. In San Jose, I was tasked to investigate crimes against children, white collar, and intellectual property investigations. I have been assigned to the Juneau Resident Agency within the Anchorage Division of the FBI since April of 2018. In my current assignment, I am responsible to investigate all criminal activity currently under the jurisdiction of the FBI to include investigations into various crimes against children.

2. Due to the proliferation of technical resources in criminal activity, particularly the use of computers, smart phones, and other digital devices, I have investigative experience with technical aspects of criminal investigations, and I have attended trainings, conferences, and seminars that have provided me training on technical resources.
3. Based on my training and experience, individuals who participate in the grooming of minors oftentimes possess, distribute, and produce child pornography. Further, based on my training and experience, those who engage in sending obscene images, typically do so with the expectation of a similar image returned in exchange.
4. The information contained in this affidavit is derived from my own personal knowledge and experience, and from other law enforcement and non-law enforcement personnel.
5. This search seeks evidence, fruits, and instrumentalities relating to violations of the following statutes:
    a. 18 U.S.C. § 1470, Transfer of Obscene Material to Minors;
    b. 18 U.S.C. § 2251(a), Production of Child Pornography;
    c. 18 U.S.C. § 2252(a)(4)(B), Possession of Child Pornography; and
    d. 18 U.S.C. § 2422(b), Coercion and Enticement and Attempted Coercion and Enticement of a Minor;
    e. 21 U.S.C. § 841(a)(1), Distribution of a Controlled Substance.

PROPERTY TO BE SEARCHED

6. This affidavit is made in support of an application for a warrant to search of a Black Smartphone w/ UB Pro Case ("**DEVICE 1**"- FBI Evidence Item 1B-6), Blackberry cellular telephone ("**DEVICE 2**"- FBI Evidence Item 1B-7), AT&T prepaid SIM card 89014103271599703368 ("**SIM CARD 1**") and AT&T pre-paid SIM card

8901410327178942538 ("**SIM CARD 2**"). (*SIM CARD 1 and 2 are both maintained as FBI Evidence Item 1-B7*). From hereinafter all four devices will be collectively referred to as "**SUBJECT DEVICES**", which is described in Attachment A (attached hereto and incorporated herein by this reference).

7. The SUBJECT DEVICES were seized subsequent to the arrest of Jose Rodriguez (RODRIGUEZ), date of birth May 13, 1990, on March 11, 2020 pursuant to a Federal Arrest Warrant; Warrant 1:20-mj-00021-MMS.

8. Since this affidavit is being submitted for the limited purpose of securing a warrant to search and seize the items specified in Attachment B (attached hereto and incorporated herein by this reference), which constitutes evidence, fruits or instrumentalities of violations or attempted violations of 18 U.S.C. §§ 1470, 2251(a), 2252(a)(4)(B), and 2422(b) and 21 U.S.C. § 841(a)(1) from the aforementioned property, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish a foundation for the requested search warrant. The relevant statutory authority and terms used in this affidavit and its attachments are described and defined below.

RELEVANT STATUTES

9. The following statute is relevant to this application:

   a. Title 18 U.S.C. § 1470 provides, in relevant part, Whoever, using the mail or any facility or means of interstate commerce, knowingly transfers obscene matter to another individual who has not attained the age of 16 years, knowing that such

other individual has not attained the age of 16 years, or attempts to do so, shall be fined under this title.

b. Title 18 U.S.C. § 2251(a) provides, in relevant part, Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

c. Title 18 U.S.C. §§ 2252(a)(4)(B) provide, in relevant part, that any person who knowingly possesses, or knowingly accesses with intent to view any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been so

transported, by any means including by computer, if (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct, or any person who attempts to do so, shall be guilty of a federal offense.

d. Title 18 U.S.C. § 2422(b), prohibits using the mail or any facility of interstate of foreign commerce, to knowingly persuade, induce, entice, or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged with a criminal offense, or attempt to do so.

e. Title 21 U.S.C § 841(a)(1), states that, [e]xcept as authorized by this subchapter, it shall be unlawful for any person knowingly or intentionally-(1)to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance. Title 21 U.S.C. § 859 generally doubles the maximum punishment for anyone convicted of distributing controlled substance to a person under the age of 21.

DEFINITIONS

10. The following terms are relevant to this affidavit in support of this application for a search warrant:

a. *Capture:* With respect to an image, means videotape, photograph, film, record by any means, or broadcast. *See* 18 U.S.C. § 1801(b)(1).

b. *Child Erotica:* The term "child erotica" means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings,

letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.

c. *Child Pornography:* The term "child pornography" is defined at 18 U.S.C. § 2256(8). It consists of visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252 and 2256(2), (8).

d. *Minor:* The term "minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. *Private Area of Individual:* As used in Title 18 U.S.C. § 1801(a), the term means the naked or undergarment clad genitals, pubic area, buttocks, or female breast of that individual. *See* 18 U.S.C. § 1801(b)(1).

f. *Sexually Explicit Conduct:* The term "sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

g. *Under Circumstances in Which That Individual has a Reasonable Expectation of Privacy:* As used in Title 18 U.S.C. § 1801(a) means (A) circumstances in which a reasonable person would believe that he or she could disrobe in privacy, without being concerned that an image of a private area of the individual was being captured; or (B) circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or private place. *See* 18 U.S.C. § 1801(b)(1).

h. *Visual Depictions:* "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

11. The following technical terms are relevant Affiant's affidavit in support of this application for a search warrant.

a. As part of Affiant's training, Affiant has become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers[1] and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including cellular networks and satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other

[1] The term "computer" is defined by 18 U.S.C. § 1030 (e) (1) to mean "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail").

b. Set forth below are an alphabetical listing of some definitions of technical terms, used throughout this Affidavit, and in Attachments A and B, hereto, pertaining to the Internet and computers more generally.

i. *Compressed file*: A "compressed file" is a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

ii. *Computer system and related peripherals, and computer media*: As used in this Affidavit, the terms "computer system and related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, in addition to computer photographs, and other visual depictions of such graphic interchange formats, including but not limited to, JPG, GIF, TIF, AVI, and MPEG.

iii. *Digital device*: A "digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including central processing units; desktop, laptop or notebook computers; tablets, internet-capable cellular phones (smart phones), or personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, flash drives, thumb drives, floppy disks, compact disks, DVDs, magnetic tapes, and memory chips; and security devices.

iv. *Hash value*: A "hash value" is a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data. The term "SHA-1" or "SHA-1 hash" refers to a type of hash value that may be given to a computer file. The SHA-1 is a cryptographic hash function designed by the United States National Security Agency and is a United States Federal Information Processing Standard. SHA stands for "secure hash algorithm." SHA-1 hash value is the standard for unique identifying numbers. It is computationally infeasible for two files with different content to have the same hash values. I am unaware of any instance in which two files have been naturally assigned the same SHA-1 hash value.

v. *Image or copy*: An "image or copy" is an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

vi. *Log files*: "Log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a web site was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

vii. *Malicious Software ("malware")*: Software designed to infiltrate a computer without the owner's informed consent is called "malicious software" or "malware." The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.

viii. *Metadata*: "Metadata" are data contained in a file that is not usually associated with the content of a file but is often associated with the properties of the application or device that created that file. For example, a digital camera photograph often has hidden data that contains information identifying the camera that manufactured it and the date the image was taken.

ix. *Steganography*: "Steganography" is the art and science of communicating in a way that hides the existence of the communication. Within the computer world, it can be used to hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.

c. The terms "*records*" and "*information*" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writings, drawings or paintings); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

COMPUTERS AND CHILD PORNOGRAPHY

12. Based upon Affiant's training and experience as well as discussions with others involved in child pornography investigations, computers and computer

technology have revolutionized the way in which child pornography is produced, distributed, received and possessed.

13. Through the use of computers and the Internet, distributors of child pornography use various distribution networks, including but not limited to, personal email contacts, file-sharing services, list serves, and membership-based/subscription-based web sites to conduct business, allowing them to remain relatively anonymous.

14. The development of computers has also revolutionized the way in which child pornography collectors interact with each other, and sexually exploit children. Computers serve four basic functions in connection with child pornography: production, communication and distribution, and storage. More specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

    a. Production: Producers of child pornography can now produce high resolution still and moving images directly from a common video or digital camera, to include cellphones with built in cameras. In this day and age, these types of cameras have become ubiquitous, and are located on nearly every cell phone sold. Once taken, images and videos can be saved onto a computer or uploaded onto a website or attached to an email within seconds. While still on the camera or after being saved onto a computer or uploaded into a photo or video editing program, images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. Videos can be edited, or spliced together to create montages of abuse that can be several minutes to several hours long. As a result of this technology, it is relatively inexpensive and

technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow. In some cases, depending upon the sophistication of the producer, it may be virtually impossible to law enforcement to determine the source of a sexually explicit image.

b. Communication and Distribution: The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. In addition, the Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer to look for "footprints" of the web sites and images accessed by the recipient.

c. Storage: The computer's capability to store images in digital form makes it an ideal repository for child pornography. It is not uncommon to find cellphones with 32 gigabytes (GB) or more of data. Many cellphones also have expandable external storage in the form of SD cards or other storage devices. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 1 terabyte are not uncommon. These drives can store thousands of images at very high resolution. Storage options located outside the physical boundaries of a computer add another dimension to the equation. According to www.avforums.com, 1 GB of data equates to approximately 20 minutes of high definition video.

d. Child pornographers can now transfer photographs onto a computer directly from a digital camera, cellphone, or from a regular camera by using a scanner. A computer's electronic storage media (commonly referred to as the hard drive) can store tens of thousands of images at a very high resolution. In addition, magnetic storage located in host computers makes it possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image in another country. Once done, there is no readily apparent evidence at the "scene of the crime." Only careful laboratory examination of electronic storage devices can recreate the evidence trail.

15. Collectors and distributors of child pornography can set up an account with a remote computing service that provides e-mail services and electronic file storage. Evidence of such online storage of child pornography may be found on the user's computer.

16. Information can be saved or stored on a computer intentionally. For example, a person may save an e-mail as a file or may save a favorite website in a "bookmark" type file. Information can also be retained unintentionally. For example, traces of an electronic communication path may be stored automatically in temporary files or Internet Service Provider client software. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Internet distributors and recipients of child pornography may be identified by examining the recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient. A forensic examiner often also can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded.

17. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or viewed via the Internet. Even when such files have been deleted, they can often be recovered by forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside for long periods of time in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space (free space or slack space). In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser

typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

//

INDIVIDUALS WITH A SEXUAL INTEREST IN MINORS

18. My knowledge of preferential sex offenders and their characteristics is based on my experience as an FBI agent, and other training specific to child exploitation crimes and related computer storage that I have received. Based upon such training and experience, as well as upon information provided to me by other law enforcement officers, I am aware of the following general characteristics, which may be exhibited in varying combinations:

    a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity.

    b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videos, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and

gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as on a cell phone that is password protected and on their person, a computer hard drive, or separate digital media.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, e-mail addresses or telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. The result is that individuals may travel with some or all of their collections, and that evidence of an individual's interest in child pornography may be located in their work places or vehicles. This is particularly true given the fact that most individuals own and keep on their person or close by their cell phones (with their significant storage capacities). In addition, the portable nature of many laptops computers, tablets,

and storage devices also allow for easy transport between and individuals home and their ultimate destination.

NARCOTICS TRAFFICKING

19. Based on my training, experience and participation in these and other financial/drug trafficking investigations, and based on my conversations with other experienced law enforcement agents, officers, and prosecutors with whom I work, I know the following:

20. In my experience, I have found that the distribution of controlled substances is frequently a continuing activity over months and years. Persons involved in the trafficking of illegal controlled substances typically will obtain and distribute controlled substances on a regular basis, much as a distributor of a legal commodity would purchase stock for sale. Similarly, such drug traffickers will maintain an "inventory" which will fluctuate in size depending upon the demand for and the available supply of the product.

21. It has been my experience that drug traffickers keep records of their illegal activities not only during the period of their drug trafficking violations but also for a period of time extending beyond the time during which the trafficker actually possesses/controls illegal controlled substances. The records are kept in order to maintain contact with criminal associates for future transactions and so that the trafficker can have records of prior transactions for which the trafficker might still be owed money or might owe someone else money. Such records may be found in the form of text messages, or other digital files, on wireless telephones.

22. It is common for members of drug trafficking organizations to maintain records evidencing their illegal activities including books, ledgers, receipts, notes and other

papers relating to the transportation, ordering, possession sale and distribution of drugs and the collection and transportation of drug proceeds. I also know that the aforementioned records are frequently maintained in the drug trafficker's wireless telephones.

23. I know that evidence of excessive wealth is probative evidence of crimes involving greed, to include the distribution of controlled substances. Therefore, receipts showing the expenditure of large sums of money and/or the expensive assets themselves is evidence of drug trafficking. I also know that drug traffickers commonly keep the expensive assets themselves and/or documentation of the purchase of the asset (receipts, warranty cards, etc.) sometimes store documentation or photographs of these assets in their wireless telephones.

24. It is increasingly common for members of drug trafficking organizations to utilize direct cash deposits into a co-conspirator's bank accounts to facilitate the movement of US currency throughout the trafficking organization's area of operations. I know that members of drug trafficking organizations will utilize nominee depositors to disguise the origination of the funds and to break up the amount being deposited by any one person. I know that the actual owner of the currency will commonly provide the nominee depositor with hand-written information concerning the intended recipients name, account number, and amounts of money to be deposited. I also know that, in an attempt to keep track of the proceeds, it is common for the drug traffickers and/or nominee depositors to maintain copies of the deposit slips. I also know that the aforementioned items are frequently maintained in a drug trafficker's and/or nominee depositor's wireless telephones.

25. It is common for members of drug trafficking organizations to utilize fraudulent identification, in order to purchase airline tickets, send wire transfers, rent residences and storage facilities and subscribe for telephone/cellular telephone service. I also know it is common for drug traffickers to keep fraudulent identification nearby and easily accessible to facilitate their flight upon the discovery of their illegal activities by law enforcement. I also know records concerning the purchase of airline tickets, rental contracts, and cellular service are frequently found on wireless telephones.

26. It is common for drug trafficking organizations involved in the distribution of controlled substances to maintain equipment and supplies (i.e. scales, baggies, cutting agents) on hand over a lengthy period of time. At times, certain retail stores provide customers with loyalty cards that can track a customer's purchases. Frequently, these stores send emails to the members of their loyalty programs that can be found on drug traffickers' wireless telephones.

27. It is common for members of drug trafficking organizations to attempt to recruit couriers to transport drugs and/or US currency throughout the trafficking organization's area of operations. I know that often times the couriers' handler will send the courier with messages regarding travel itinerary, hotel information and contact telephone numbers prior to the courier departing on the trip to transport drugs and/or money. I also know that often times the organizations will pay a flat rate (i.e. $2,000 per ounce for heroin) plus expenses for the couriers. Therefore, often times the couriers will keep itemized lists of expenses and/or receipts, in order to be reimbursed. The aforementioned evidence is frequently maintained in the courier's wireless telephone. In addition, records of airline and hotel purchases are frequently found in email on drug

traffickers' wireless telephones. Evidence of visiting travel websites can often be found through forensic analysis of these devices.

28. It is common for members of drug trafficking organizations to take or cause to be taken, photographs and/or videos of themselves and their co-conspirators and associates. It is also common for members of drug trafficking organizations to take or cause to be taken, photographs and/or videos of themselves and/or their co-conspirators with controlled substances, large sums of money, firearms, and expensive assets (i.e. jewelry, luxury cars). I also know photographs and video footage are frequently maintained in the drug trafficker's wireless telephones.

FACTS IN SUPPORT OF PROBABLE CAUSE

Information Relating to COMPLAINANT

29. In December 2019, Affiant reviewed information from the Hoonah Police Department; Case 19-0227. In summary, on or about March 10, 2019, the Hoonah Police Department received information that RODRIGUEZ, was furnishing alcohol to minors and engaging in activities with those minors consistent with "grooming" them for sexual activity.

30. The investigation was initiated as a result of the interview of a 14-year-old female minor (COMPLAINANT) who provided information during a February 22, 2019, forensic interview conducted by the Child Advocacy Center (CAC) in Juneau, Alaska.

31. During the interview, the COMPLAINANT said the following:

a. RODRIGUEZ was living with her and her mother. RODRIGUEZ and the COMPLAINANT began talking to one another as what the COMPLAINANT viewed as a friendship. They spoke both in-person and via text message exchanges.

b. At several unknown times, RODRIGUEZ told the COMPLAINANT that he liked her more than a friend and made comments about her looks. RODRIGUEZ also offered for the COMPLAINANT to smoke marijuana and vape with him. COMPLAINANT advised RODGRIGUEZ was also purchasing alcohol for other minors in Hoonah.

c. COMPLAINANT said that in addition to herself, she heard rumors that RODRIGUEZ was "trying to get with" two other minor females, ages 14 (hereinafter "POSSIBLE VICTIM 1") and 16 (hereinafter "POSSIBLE VICTIM 2") in the Hoonah area. Based on Affiant's training and experience, "trying to get with" is slang for attempting to have relations of a sexual nature and/or engage in a romantic relationship with another individual.

d. COMPLAINANT said RODRIGUEZ told POSSIBLE VICTIM 2 he wanted to marry her. Based on the investigation to date, your Affiant is not aware if POSSIBLE VICTIMS 1 and 2 have been identified.

e. COMPLAINANT was also aware of RODRIGUEZ sending a nude photo of himself through a text message to a 14-year-old minor female (hereinafter "VICTIM 1") at some point between June and July 2018.

32. The COMPLAINANT advised she still had a text message exchange saved on her phone where RODRIGUEZ stated that he liked her. Subsequent to the interview, she provided a copy of screenshots from that exchange to law enforcement. The date of this text message exchange is unknown. The content of the exchange is as follows;

COMPLAINANT- "I don't know"
RODRIGUEZ- "What do you mean you don't know/Sorry to say this but I do/But I'm with your moms"
COMPLAINANT- "You do what?"
RODRIGUEZ- "And you are not my age"

COMPLAINANT- "What?"
RODRIGUEZ- "Nothing"
COMPLAINANT- "Okay"
RODRIGUEZ - "Like you"
COMPLAINANT - "Oh okay"
RODRIGUEZ- "You don't"
COMPLAINANT- "I like you as a friend"
RODRIGUEZ- "I know that I'm not saying anything"
COMPLAINANT- "Okay"
RODRIGUEZ- "Erase the texts"
COMPLAINANT- "Okay i will"

Investigation of Other Possible Victims and Victim 1

33. During the investigation, the Hoonah Police Department interviewed five of the minors and VICTIM 1 previously identified by the COMPLAINANT as minors who RODGRIGUEZ was purchasing alcohol for. Except for VICTIM 1, none of the minors, both male and female, disclosed RODRIGUEZ ever bought them alcohol or made comments of a sexual nature towards them.

34. One of the minors interviewed was a 16-year-old female. During the interview, she admitted to drinking alcohol, but was not forthcoming with the Hoonah Police Officer as to how she was able to obtain it. She also stated she did not know who RODRIGUEZ was. The 16-year-old minor was interviewed in the presence of her mother. Based on Affiant's training and experience, your Affiant knows that individuals who are interviewed in the presence of others; such as a parent, a spouse, or a manager, are not always forthcoming. This is due to the fact they believe if they provide truthful information, they might be embarrassed and/or concerned about the possible repercussions of being forthcoming.

35. On or about March 15, 2019, VICTIM 1 was initially interviewed. VICTIM 1 said the following:

a. VICTIM 1 said she did not drink alcohol but knew of other minors who did. VICTIM 1 was not aware of who bought the alcohol for the other minors.

b. VICTIM 1 was familiar with who RODRIGUEZ was and stated the two of them had exchanged text messages. VICTIM 1 advised RODRIGUEZ told her she was beautiful, pretty, and wanted to smoke marijuana with her. VICTIM 1 advised she told RODRIGUEZ how old she was. RODRIGUEZ knew she was friends with COMPLAINANT 1, who was a similar age.

c. VICTIM 1 advised RODRIGUEZ sent VICTIM 1 photos of himself. The photos were of himself shirtless and a photo of his private parts. VICTIM 1 advised she deleted all the images and text message he sent her during the summer of 2018, but still had the phone that she used at the time in her possession.

36. VICTIM 1's phone was provided to the Hoonah Police Department and sent to the Alaska Department of Public Safety Technical Crimes Unit for processing. On July 1, 2019, the cellular telephone provided by VICTIM 1 was examined by the Alaska Department of Public Safety Technical Crimes Unit. The results of the examination determined the cellular telephone had been factory reset prior to being provided to law enforcement. As a result of this factory reset, no items of evidentiary value were found.

Recorded Phone Call between RODRIGUEZ and VICTIM 1

37. Based on the information provided by VICTIM 1, an Officer with the Hoonah Police Department applied for and was granted a *Glass* Warrant, Warrant #1HN-19-01SW, to record a conversation between VICTIM 1 and RODRIGUEZ on March 15, 2019.

38. On March 15, 2019, a phone call was placed to RODRIGUEZ, telephone number (907) 612-1105, by VICTIM 1. During the call, VICTIM 1 asked the person who answered the phone "is this Jose?" and the individual responded, "Uh huh." VICTIM 1 then identified herself, stated she needed his help, and asked him if he remembered the naked pictures he sent her this summer. The individual

again replied "Uh huh." VICTIM 1 stated that her mother was snooping around, and she wanted to delete the photos from her phone so her mother wouldn't find out. The individual replied "Alright." The call continues and the individual eventually appears to hang up the phone.

39. Hoonah Police was able to confirm the telephone number (907) 612-1105 was utilized by RODRIGUEZ after conferring with COMPLAINANT 1's parents, who advised this was the number RODRIGUEZ used. Additionally, this telephone number appeared in VICTIM 1's cellular telephone provider's billing records which were provided by VICTIM 1's parent. These records contained logs of multiple text message exchanges on July 24, 2019 and July 25, 2019, between VICTIM 1 and telephone number (907) 612-1105.

40. On March 15, 2019, a Search Warrant, Warrant #1HN-19-02SW, was obtained for RODRIGUEZ's cellular telephone (hereinafter "LG SMARTPHONE") The Hoonah Police Department contacted RODRIGUEZ at his residence. After making contact, RODRIGUEZ was asked if his number was (907) 612-1105 and he replied, "Uh Huh." The LG SMARTPHONE was subsequently seized and sent to the Alaska Department of Public Safety Technical Crimes unit to be analyzed.[2]

41. The Affiant reviewed the Alaska Department of Public Safety Technical Crimes Unit reports related to the examination of the LG SMARTPHONE. In the report, multiple photos of a male individual, believed to be RODRIGUEZ, were seized. There were multiple photos of the male individual shirtless, which was the description of one of the photos described by VICTIM 1. Multiple photos of a male genitalia were also found and seized. Lastly, an image with a Puerto Rican identification card for RODRIGUEZ was seized from the LG SMARTPHONE. No text messages of

[2] It should be noted the Honorable State Judge Mary Kay Germain restricted the scope of Search Warrant #1HN-19-02SW for investigators to review text message exchanges between the dates of July 24, 2018 and July 25, 2018. Based on your Affiant's review of the toll records, which only outlined toll records from June 26, 2018 through July 26, 2018, the Affiant believes the scope of this search was restricted to this date range due to the fact that VICTIM 1's toll records, which were copies provided by VICTIM 1's parents, appeared to only show contacts with telephone number (907) 612-1105 on July 24, 2018, and July 25, 2018.

investigative interest were seized during the allotted timeframe outlined in Warrant #1HN-19-02SW, and no images of underage females were observed.

42. The Technical Crimes Unit Investigator further advised there were in excess of over 1,000 text messages on the SUBJECT DEVICE that were not searched due to the temporal restriction imposed as part of Search Warrant #1HN-19-02SW. The Investigator advised the multiple pictures of the male genitalia could have been sent in text messages, but it is unknown at this time due to the fact the text messages outside of the limited date range authorized by Search Warrant #1HN-19-02SW were not examined.

43. On July 12, 2019, the Hoonah Police Department took several of the images located on the SUBJECT DEVICE for VICTIM 1 to review. Approximately 5 photos were shown to VICTIM 1. The images that included male genitalia were redacted due to the age of VICTIM 1. VICTIM 1 advised RODRIGUEZ sent her a total of two photos, and she recognized one of those images from the group of 5 shown to her. The photo showed a male's stomach, hand, and redacted genitalia. The male has distinctive tattoos on his stomach and hand. In the background of the photo was a stuffed Sponge Bob Square Pants doll. At this time, it is unknown if the tattoos in the photo have been compared to the tattoos on RODRIGUEZ's person.

44. On February 6, 2020, your Affiant received subpoena returns from AT&T for phone number connected to the phone seized from RODRIGUEZ pursuant to Search Warrant #1HN-19-02SW. The number is believed to belong to RODRIGUEZ, and for the phone number connected to VICTIM 1's phone. These records were more complete than those originally provided by VICTIM 1's parents and reviewed by Hoonah Police prior to seeking Search Warrant #1HN-19-02SW. The first identified communication between RODRIGUEZ and VICTIM 1's phone was on July 24, 2018. The last

communication was on August 10, 2018. These records show over 700 text message exchanges between the two phone numbers during the noted time period.

45. Based on Affiant's review of the Hoonah Police Department's investigation, the Hoonah Police Department did not have the AT&T toll records at the time they applied for Search Warrant #1HN-19-02SW, which included additional contacts between RODRIGUEZ and VICTIM 1 in August 2018.

46. On February 7, 2020, Affiant applied for and was granted a Search Warrant for the LG SMARTPHONE; Search Warrant 1:20-mj-00009-MMS. The scope of this warrant was to search and seize the items which constituted evidence, fruits or instrumentalities of violations or attempted violations of 18 U.S.C. §§ 1470 and 2422(b) from the LG SMARTPHONE.

47. On February 20, 2020, the LG SMARTPHONE was provided to the FBI Anchorage Division's Computer Analysis Response Team (CART) Forensic Examiner for further extraction and review.

48. In reviewing the LG SMARTPHONE for images and text messages which constituted evidence, fruits or instrumentalities of violations or attempted violations of 18 U.S.C. §§ 1470 and 2422(b) from the SUBJECT DEVICE, the Forensic Examiner observed the following;

a. One thumbnail image believed to be child pornography. The image was described to affiant as an image of a prepubescent female's head and nude partial torso with her hand holding an adult male's penis with what appears to be semen running down it. Behind the prepubescent female appears to be the end of a bed and other bedroom furniture. No other part of the male is visible. The file path of the image reflects being stored as a cache file of Google Chrome. Based on my training and experience, the file path

indicates the image was likely obtained from the internet or other remote source. No further analysis of the image was completed.

b. A second thumbnail image believed to be possible child pornography. The image was described to the affiant as an image of what appears to be a prepubescent female's vagina penetrated by the top of an adult male's penis, with only the body of the penis visible. Overlaid onto the front of the vagina are large animated eyes and long dark hair tied in a "pigtail" on the side.

c. A third thumbnail image believed to be possible child pornography or child erotica. The image was described to the affiant as including two prepubescent females, one fully nude and one only wearing a shirt with the bottom half of her body possibly naked but difficult to confirm. Standing behind the two prepubescent females is a possible adult male, fully clothed and with only the left side of his body viewable from below the chest to his foot. The head and face of adult is not included in the image. Two additional thumbnail images of these same two prepubescent girls appearing to be of a series were noted directly next to this image. No further analysis of the image was completed.

d. Multiple images of marijuana, drug paraphernalia, U.S. currency, and firearms.

e. Multiple text messages of what appears to be user of the LG SMARTPHONE and others currently unknown discussing the sale of controlled substances.

49. On February 27, 2020, a rollover Search Warrant request was sent the Court to amend Search Warrant 1:20-mj-00009-MMS. The rollover request sought to include searches for items which constituted evidence, fruits or instrumentalities of violations or attempted violations of 18 U.S.C. §§ 1470, 2251(a), 2252(a)(1), 2252(a)(4)(B), and 2422(b) and 21 U.S.C. § 841(a)(1). On February 28, 2019, the court granted the rollover Search Warrant, Search Warrant 1:20-mj-00017-MMS.

50. On March 2 and 3, 2020, I reviewed the LG SMARTPHONE from RODRIGUEZ. In summary, I observed the following;

a. One image of what appeared to be consistent with the groin area of a female toddler with the vagina exposed. Also included in the image was what appeared to an adult finger and a man's penis either penetrating the vagina or anus of the toddler. The image was subsequently compared to a database of known child pornography images by an FBI Forensic Examiner, but this image did not yield a result as a known child pornography image. This image was located in cached space on the phone, and appeared to have been accessed through the Google Chrome browser.

b. One image of what appeared to be a partially nude, female wearing a blue shirt, who appeared between the age of 12 to 16 years old, with what appeared to be semen around her mouth. In the background of the image is what appears to be an adult male. The image was subsequently compared to a database of known child pornography images by an FBI Forensic Examiner, but this image did not yield a result as a known child pornography image.

c. Multiple URLs specific to pornography related to "Teens."

d. Multiple images of unknown, clothed females who appear to be between the ages of 15-20 years of age.

e. Multiple images and videos of adult pornography.

f. Multiple images of RODRIGUEZ to include the image of RODRIGUEZ's penis that was recognized by VICTIM 1. It should be noted that in this unredacted image, the visible penis contains a distinctive triangle-shaped birthmark that would be readily apparent to any individual who viewed the image.

g. Multiple text messages related to the distribution of marijuana, images of what appeared to be marijuana including individually packaged for distribution, multiple images of U.S. and foreign currency, and firearms.

51. Affiant reviewed the potential child pornography/child erotica images originally described to him by the FBI Forensic examiner on February 20, 2020. A summary from the review of the images is as follows;

a. The image was described to affiant as an image of a prepubescent female's head and nude partial torso with her hand holding an adult male's penis with what appears to be semen running down it. The image was reviewed by the affiant and it appeared to be of an adult female who exhibited the physical characteristics of a prepubescent child.

b. The image described to the affiant as an image of what appears to be a prepubescent female's vagina penetrated by the top of an adult male's penis, with only the body of the penis visible. Overlaid onto the front of the vagina are large animated eyes and long dark hair tied in a "pigtail" on the side. The image was reviewed by affiant and appeared to be consistent with child pornography. The image was subsequently compared to a database of known child pornography images by an FBI Forensic Examiner, but this image did not yield a result as a known child pornography image.

c. The image described to the affiant as including two prepubescent females, one fully nude and one only wearing a shirt with the bottom half of her body possibly naked but difficult to confirm. Standing behind the two prepubescent females is a possible adult male, fully clothed and with only the left side of his body viewable from below the chest to his foot. The head and face of adult is not included in the image. The affiant reviewed these images and they appear to be of either RODRIGUEZ's children and/or family members,

or possibly the children of RODRIGUEZ's girlfriend at the time. Other photos of the same children in clothing, and partial clothing, were also observed. This image, and other similar images of the children, were subsequently compared to a database of known child pornography images by an FBI Forensic Examiner. These images did not yield a result as known child pornography images.

52. On March 4, 2020, an FBI Forensic Examiner submitted all images and videos on the LG SMARTPHONE through a forensic tool designed to identify known child pornography images based on hash values. The results of this search yielded one known child pornography image. The FBI Forensic Examiner described the known image as the backside of a female and the image was part of a known series. It should be noted that the FBI Forensic Examiner who submitted the images through the forensic tool is not the same FBI Forensic Examiner who originally reviewed the LG SMARTPHONE on February 20, 2020.

Arrest of Jose Rodriguez

53. On March 11, 2020, RODRIGUEZ was arrested pursuant to an authorized Federal Warrant, Arrest Warrant 1:20-MJ-0021-MMS. After RODRIGUEZ was taken into custody, his personal items were identified and collected. The items collected were one Black Smartphone w/ UB Pro Case and charging cord (**DEVICE 1**), one pink and black backpack, one camouflage backpack, a wallet with RODRIGUEZ' identification inside, and a Ruger 7 mm rifle. These items were brought back to the Hoonah Police Department where RODRIGUEZ was held pending transport back to Juneau, Alaska for his initial appearance.

54. After being provided with Miranda Warnings, RODRIGUEZ advised he understood his rights and was willing to speak with investigators. During the interview, RODRIGUEZ advised he was not into child pornography, he did not view child pornography, and he did not download any onto any of

his electronic devices. RODRIGUEZ advised there were photos on his cellphone of his partially nude nieces and nephews, but RODRIGUEZ advised those photos were not pornography.

55. During the interview, RODRIGUEZ was advised of the two backpacks were seized from the residence where he was arrested. RODRIGUEZ confirmed the backpacks belong to him and consented to having them searched. During the search of the backpacks, a Blackberry Cellphone (**DEVICE 2**) and .223 round were located and seized.

56. RODRIGUEZ provided consent for his girlfriend/fiancé to take possession of his personal items, including his wallet. When investigators opened the wallet to retrieve RODRIGUEZ' identification card as requested; two SIM cards were observed; AT&T prepaid SIM cards-8901410327159970336 8 (**SIM CARD 1**) and 8901410327178942538 4 (**SIM CARD 2**). SIM CARD 1 and SIM CARD 2 were subsequently seized.

Indications of Possible Other Digital Devices

57. Affiant was unable to locate communications between RODRIGUEZ and VICTIM 1 on the LG SMARTPHONE. Based on Affiant's review of the LG SMARTPHONE and the aforementioned AT&T records, it is Affiant's belief the LG SMARTPHONE was not the cellular telephone originally used for the text message exchanges based on the following;

a. During the review, Affiant observed several images featuring RODRIGUEZ and at least two different cellular telephones which do not appear to match the LG SMARTPHONE currently in the FBI's custody.

b. Text message activity appear to begin after September 2018, which is subsequent to the contacts described by VICTIM 1.

c. The AT&T records indicate the make and model of the phone used during the July 24, 2018, through August 10, 2018, text exchanges between RODRIGUEZ and VICTIM 1 differs from the make and model of the LG SMARTPHONE.

d. The image identified by VICTIM 1 and observed on the LG SMARTPHONE appears to have been created on March 31, 2018, and taken by another device. This device model number differed from both the LG SMARTPHONE and the device referenced in the AT&T records.

58. RODRIGUEZ's appeared to utilize pre-paid phone accounts. Based on my training experience, I know that people who use pre-paid phone accounts regularly exchange phones. I also know that data can be transferred from one phone to the other with the use of SD cards or back-up from a cloud server. Various types of data can be transferred based on the user's preference and/or the phone's operating system. Conversely, information can also be chosen not to transfer over, such as deleted text messages, to the new phone.

59. Affiant is also aware that SD cards used in Android smartphones, the same type of smartphone previously seized from RODRIGUEZ on March 15, 2019 by the Hoonah Police Department, store data such as contact information and text message exchanges.

60. Based on my training and experience, I know that individuals who engage in drug trafficking, and/or who engage sexual grooming and courting, use prepaid telephones to conceal their activities from both law enforcement and/or their significant others.

Summary of Probable Cause

61. This search warrant seeks authorization to search the DEVICE 1, SEVICE 2, SIM CARD 1, and SIM CARD 2 (hereinafter- **SUBJECT DEVICES**) for evidence, fruits or instrumentalities of violations or attempted violations of 18 U.S.C. § 1470, 2252(a)(1),

2252(a)(4)(B), and 2422(b) and 21 U.S.C § 841(a)(1). Each of these crimes generally relates to the sexual exploitation of minors and distribution of controlled substances. I submit that there is probable cause to search the SUBJECT DEVICES for the following reasons:

a. Communications between Victim 1 and RODRIGUEZ occurred between July 24, 2018, and approximately August 10, 2018. During this time, VICTIM 1 stated that RODRIGUEZ sent her a photograph with his exposed genitalia. VICTIM 1 has identified this photograph among those photographs located on the SUBJECT DEVICE. VICTIM 1 also described RODRIGUEZ's statements about VICTIM 1 being beautiful and pretty, and described that RODRIGUEZ had offered her marijuana. In Affiant's training and experience, each of these actions is consistent with RODRIGUEZ attempting to groom VICTIM 1 to engage with him in sexually explicit conduct.

b. Additional evidence supports the conclusion that RODRIGUEZ has a sexual interest in minors consistent with him sending an image of his genitalia to a minor that he was attempting to groom. That evidence includes:

   i. COMPLAINANT described RODRIGUEZ making multiple statements about liking her more than as a friend and "trying to get with" her. COMPLAINANT also provide law enforcement with text messages in which RODRIGUEZ told COMPLAINANT that he liked her, and also instructed her to erase the record of that communication.

   ii. The search of the LG SMARTPHONE; Search Warrant 1:20-MJ-00017-MMS, yielded multiple images, videos, and URL links related to "Teen" pornography. Affiant observed multiple images of clothed females who

appeared to be between the ages of 15 to 20 years of age. In addition, one image on the SUBJECT DEVICE was identified as child pornography, and three additional images are suspected. Based on my training and experience, individuals who view this type of material, are demonstrating a sexual interest in minors or minors who appear to be minors.

c. Text messages and images observed by the FBI Forensic Examiner and Affiant appear to corroborate the COMPLAINANT's information RODRIGUEZ was involved with the distribution of marijuana and/or other controlled substances.

d. Affiant has reviewed RODRIGUEZ's criminal history. RODRIGUEZ has previous convictions for drug-related distribution offenses which appear to be connected with distributing controlled substances to minors.

e. . Based on my training experience, I know that people who use pre-paid phone accounts regularly exchange phones. I also know that data can be transferred from one phone to the other with the use of SD cards. SD cards can store data such as contact information and text message exchanges.

SPECIFIC METHODS OF SEARCHING FOR DIGITAL EVIDENCE

62. I am seeking authority to search for, among other things, items containing digital data, more particularly described in Attachment B. Consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire

medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

63. The search of a computer hard drive or other computer storage medium is a time-consuming manual process often requiring months of work. This is so for a number of reasons, including the complexity of computer systems, the multiple devices upon which computing can take place, and the tremendous storage capacity of modern day computers, and the use of encryption or wiping software. As explained above, modern day computers and storage devices are capable of holding massive quantities of data, and the volume of evidence seized in these cases can be immense. I am aware of cases in which individuals have possessed thousands of images on their computer, multiple computers and hard drives, or dozens of storage media upon which contraband images were found. Affiant knows from training and experience, and from discussions with trained computer forensic examiners, that a review of such quantities of evidence can take a significant amount of time. Second, there is a limited pool of personnel capable of conducting a forensic examination. Third, in some instances an individual may utilize encryption software or other publicly available techniques such as wiping software to hide their digital activity. Forensic tools are available to circumvent some of these techniques; however, these tools may require a significant allocation of resources and a substantial period of time.

64. Some or all of the following search methods may be used to conduct the forensic search in this case. These methods are not listed in any particular order, nor is their listings in this affidavit a representation that they will be used in this particular case:

a. *Keyword Searches*: I know that computer forensic utilities provide the capability for a user to search for specific key words that may exist on a piece of digital media. I intend to use specific keywords. As it concerns to the investigation

described above, examples of such keywords include, but are not limited to "Divorce," and "Domestic violence." Those keyword searches will indicate files and other areas of the hard drive that need to be further reviewed to determine if those areas contain relevant data. A list of keywords utilized will be maintained with the records of the forensic examination.

b. *Data Carving*: I know that, as previously mentioned, data residue may be left in the "free," "unallocated," or "slack" space of a computer hard drive, that is, the space not currently used by active files. I further know that, as previously mentioned, many operating systems utilize temporary storage often referred to as "swap space" on the hard drive to store contents from main system memory. Such unallocated and swap space may contain the residue of files that can be carved out, often in an automated or semi-automated fashion. I intend to use forensic tools to carve out files, in particular, image files such as JPEG and GIF files. The mere act of carving out such files does not expose me to the contents of such recovered files, but makes those files available for further relevancy checks, such as keyword searches (explained above) and hash value comparisons (explained below).

c. *Hash Value Comparisons*: I know that computer forensic utilities provide the capability to utilize a function known as a hash algorithm. A hash algorithm uses a mathematical formula to analyze the data composing a file, and to generate a unique "fingerprint" for that file. The act of hashing a piece of data does not reveal to an investigator any information about the contents of that data. However, I know that computer forensic applications often contain databases of

known hash values for files. Some of those files are "ignorable," which enables other forensic processes to ignore files (such as the Windows operating system) that are not evidentiary in nature. I seek permission to utilize automated hash value comparisons to both exclude irrelevant files, and to potentially locate relevant files. Hash value comparisons are useful, but not definitive, as even a single-bit change to a file will alter the hash value for the file. The forensic review team does not intend to rely solely on hash value comparisons, but intends to utilize them in order to assist with identifying relevant evidence. The use of this search method is intended to narrow the search. A search of known hash values, however, will not be used exclusively because I know that typically there are many files on digital devices with unknown hash values. Using a hash value search method exclusively would not uncover the data as well as other evidence authorized by this warrant and described in Attachment B.

d. *Opening Container Files, Encrypted Volumes, and Embedded Files*: I know that relevant data may be compressed, encrypted, or otherwise embedded in other files or volumes. It is often not possible through any automated process to examine the contents of such containers without opening them, just as it is not possible to examine the contents of a locked safe without first opening the safe. In the event that compressed, encrypted, or otherwise embedded files or volumes may exist on the seized items, I intend to request the use of sophisticated forensic tools to attempt to open any such container files that may reasonably contain evidence.

e. *File Header / Extension Checks*: I know that individuals involved in illegal activities or attempting to hide activities from other users on a computer often

change the extension of a file (such as .jpg) to some other incompatible extension (such as .txt) in order to disguise files from casual observers. An example of a person attempting to hide activities on a computer would be that of a domestic abuse victim attempting to hide documents related to assistance for victims. The extension of a file, however, is not necessarily linked to the "header" of a file, which is a unique marking imbedded automatically in many types of files. By comparing the extension of a file with the "header information" of a file, it is possible to detect attempts to disguise files. Such a comparison can be made in an automated process by computer forensic tools. I intend to run an automated header comparison to detect such efforts and intend to review any such files that reasonably may contain evidence authorized by this warrant.

f. *Thumbnail / Image Views*: Because the majority of the expected files will not have known hash values, a negative hash value comparison does not exclude a file. There is no known alternative for visually inspecting each file. I therefore intend to examine at least a thumbnail image of each image file on the digital media whether "live," "data carved," or identified by header as well as other files.

g. *Registry / Log File Checks*: I know that it is necessary in any criminal case to establish not only that a crime has occurred, but also to establish what person committed that crime. Operating systems and computer programs often maintain various administrative files such as logs that contain information about user activities at certain times. In the Windows operating system, for example, some of these files are collectively referred to as "the registry". Such files contain specific information about users, often including e-mail addresses used,

passwords stored, and programs executed by a particular user. These files may also contain evidence regarding storage devices that have been connected to a computer at some time. Multiple backup copies of such files may exist on a single computer. I intend to examine these files to attempt to establish the identity of any user involved in the creation, editing, or use of files found on the digital devices, and to establish methods (such as software used) and dates of this activity.

h. *Metadata / Alternative Data Streams*: I know that many file types, operating systems, and file systems have mechanisms for storing information that is not immediately visible to the end user without some effort. Metadata, for example, is data contained in a file that is not usually associated with the content of a file, but is often associated with the properties of the application or device that created that file. For example, a digital camera photograph often has hidden data that contains information identifying the camera that manufactured it, and the date the image was taken. Some file systems for computers also permit the storage of alternate data streams, whereby a file such as a text file may hide an image file that would not be immediately visible to an end user without some action taken. I know that both metadata and alternative data streams may contain information that may be relevant. Metadata and alternative data streams are often identified and processed automatically by computer forensic utilities. I intend to review any such data that is flagged by any process above as being relevant.

65. Criminal Procedure Rule 41 specifically states "The officer may retain a copy of the electronically stored information that was seized or copied." Fed. R. Crim. P. 41 (f)(1)(B).

Moreover, upon identification of contraband, the item is subject to forfeiture, and the owner has a reduced expectation of privacy in those seized devices. Consequently, should a seized device be found during the authorized forensic review to contain contraband, it will be retained by the United States, and may be searched without further authorization of the Court for the evidence described in Attachment B. Such a later search may be required for the following reasons:

a. Should the execution of the warrant uncover data that may later need to be introduced into evidence during a trial or other proceeding, the authenticity and the integrity of the evidence and the government's forensic methodology may be contested issues. Retaining copies of seized storage media may be required to prove these facts.

b. Returning the original storage medium to its owner will not allow for the preservation of that evidence. Even routine use may forever change the data it contains, alter system access times, or eliminate data stored on it.

c. Because the investigation is not yet complete, it is not possible to predict all possible defendants against whom evidence found on the storage medium might be used. That evidence might be used against persons who have no possessory interest in the storage media, or against persons yet unknown. Those defendants might be entitled to a copy of the complete storage media in discovery. Retention of a complete image assures that it will be available to all parties, including those known now and those later identified.

d. The act of destroying or returning storage medium could create an opportunity for a defendant to claim, falsely, that the destroyed or returned storage medium contained evidence favorable to him. Maintaining a copy of the storage medium

would permit the government, through an additional warrant if necessary, to investigate such a claim.

e. Similarly, should a defendant suggest an explanation for the presence of evidence on storage medium or some defense, it may be necessary to investigate such an explanation or defense by, among other things, re-examining the storage medium with that explanation or defense in mind. This may require an additional examination of the storage medium for evidence that is described in Attachment B but was not properly identified and segregated previously.

66. In the event that a piece of digital media is found not to be (a) an instrumentality of the offense, (b) a fruit of the criminal activity, (c) contraband, or (d) evidence of the offenses specified herein, it will be returned as quickly as possible.

SEALING REQUEST

67. Search Warrants 1:20-mj-00009-MMS and 1:20-mj- 00017-MMS were sealed by the Magistrate Judge in order to protect the ongoing investigation, and to avoid the unnecessary disclosure of information about minors. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. The items and information to be seized are relevant to an ongoing investigation of RODRIGUEZ. To date, law enforcement has identified an obscene image RODRIGUEZ transferred to a VICTIM 1, but does not know if that image or others have been sent to other minors. Law enforcement is also aware of child pornography on the phone searched pursuant to Search Warrants 1:20-mj-00009-MMS and 1:20-mj- 00017-MMS, but has not yet identified the individual in this image. Furthermore, law enforcement also does not know if RODRIGUEZ has been in communication with others about these incidents,

and whether or not relevant evidence may be in the possession of those individuals. Were such evidence to exist, public disclosure of this search warrant would give those individuals an opportunity to hide or destroy evidence. Withholding public disclosure of this search warrant will allow law enforcement to protect the privacy of VICTIM 1, the COMPLAINANT, and other minors who may be potential victims of RODRIGUEZ. Premature disclosure of the contents of this application and related documents may have a significant and negative impact on the continuing investigation and/or may severely jeopardize its effectiveness.

CONCLUSION

68. It is the Affiant's belief, based upon the facts contained herein and previous training and experience, that RODRIGUEZ did send at least one sexually explicit image to a minor. In addition, it is the Affiant's belief probable cause exists that RODRIGUEZ could have sent additional sexually explicit photos to minors and requested reciprocating images in exchange as outlined in the probable cause section of this affidavit. If attempts were made by RODRIGUEZ to solicit images from minor victims via text message, or other messaging platform, from the SUBJECT DEVICES, this would constitute the attempted possession, transportation, and production of child pornography

69. It is further the Affiant's belief, based upon the facts contained herein and previous training and experience, that RODRIGUEZ is involved with the distribution of controlled substances as outlined in the probable cause section of this affidavit.

70. Therefore, it is the Affiant's belief, based upon the facts contained herein and previous training and experience, that there is probable cause to believe that evidence, fruits or instrumentalities (see Attachment B, attached hereto and incorporated herein by this reference)

Jun 09 2020

of violations of 18 U.S.C. §§ 1470, 2251(a), 2252(a)(4)(B), and 2422(b) and 21 U.S.C. § 841(a)(1), are currently concealed within the SUBJECT DEVICES described in Attachment A.

FRANK D. REID, Jr.
Special Agent
Federal Bureau of Investigation

Subscribed electronically and sworn telephonically before me this 9th day of June 2020, at Anchorage, Alaska.

~~SUBSCRIBED AND SWORN TO BEFORE ME this ____ day of June 2020, at Juneau, Alaska.~~

MATTHEW M. SCOBLE
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF ALASKA